500.41092X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: Mototsugu NISHIOKA

Serial No.: 10/046,224

Filed: January 16, 2002

For: PUBLIC-KEY CRYPTOPGAPHIC SCHEMES SECURE AGAINTS AN ADAPTIVE CHOSEN CIPHERTEXT ATTACK IN THE STANDARD MODEL

Group: 2136

Examiner: D. G. Cervetti

APPEAL BRIEF

MS Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

February 7, 2007

Sir:

This Appeal is being filed in response to the decision by the Examiner in the Final Office Action dated February 7, 2006 in which claims 23-44 were finally rejected. In accordance with 37 CFR §41.37, the Appellant provides the following.

I. REAL PARTY IN INTEREST

The Real Party in Interest in this Appeal is Hitachi, Ltd., as evidenced by the Assignment filed on February 26, 2002 in Application Serial No. 10/046,224, filed January 16, 2002, said application being the subject of this Appeal, and recorded on Reel 012624 and Frame 0156.

II. RELATED APPEALS AND INTERFERENCE

There are no other Appeals or Interferences that may directly affect, may be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 23-44 are currently pending.

Claims 25-27, 29, 31-34, 37-39 and 42-44 are rejected under 35 USC §112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicants regard as their invention;

Claims 23-44 are rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter; and

Claims 23-44 are rejected under 35 U.S.C. §103(a) as being unpatentable over U. S. Patent No. 6,697,488 to Cramer et al. ("Cramer").

IV. STATUS OF AMENDMENTS

An Amendment was filed September 7, 2006 so as to amend claims 23-44 to correct the informalities noted by the Examiner, and to bring the claims into conformity with the requirements of 35 U.S.C. §112, second paragraph and 35 U.S.C. §101. In an Advisory Action mailed on September 21, 2006, the Examiner denied entry of this Amendment. Another Amendment was filed on even date herewith so as to include the amendments of the September 7, 2006 Amendment, to further amend claim 24 to overcome the 35 U.S.C. §101 rejection, and to correct a minor

informality in claim 36. Entry of this Amendment is requested as it simplifies the issues for appeal. The Appendix being submitted with the present Appeal incorporates the amendments to claims 23-44, which were filed on even date herewith. No other amendments were filed after final rejection.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The present invention as recited in the claims is directed to a public-key cryptographic method implemented in a computer, and a cryptographic communication method implemented in a computer, such as that illustrated, for example, in Figs. 4-6. The public-key cryptographic method implemented in a computer system generates a secret key and a public key by a key generation step, performs a ciphertext generation and transmission step of selecting random numbers for a plaintext, performs a ciphertext reception and decipher step of calculating from the received ciphertext by using the secret key which satisfies a particular function, outputs the deciphered results if the function is satisfied, and outputs an indication that the received ciphertext is rejected if the function is not satisfied.

Specifically, as recited in independent claim 23, the present invention as described, for example, on page 9, line 15 to page 13, line 4 of the present application, is directed to a public-key cryptographic method implemented in a computer system. The method includes a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1} {g_2}^{x_2}$, $d_1 = {g_1}^{y_{11}} {g_2}^{y_{12}}$, $d_2 = {g_1}^{y_{21}} {g_2}^{y_{22}}$, $h = {g_1}^{z}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$

The group G is a partial group of the group G', and X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

M is a plaintext space. The method also includes a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Z_q$ for a plaintext m ($m \epsilon M$), and calculating:

$$u_1 = {g_1}^{r}, \quad u_2 = {g_2}^{r}, \quad e = \pi(\alpha_1, \alpha_2, m) h^{r}, \quad v = {g_1}^{\alpha_1} c^{r} {d_1}^{\alpha r} {d_2}^{mr}$$

where $\alpha = \alpha_1 || \alpha_2$. The ciphertext generation and transmission step also includes transmitting (u_1, u_2, e, v) as a ciphertext. The method also includes a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, $m' \epsilon M$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = e / {u_1}^{z}$$

If the following is satisfied:

$${g_1}^{\alpha'_1} {u_1}^{x_1 + \alpha' y_{11} + m' y_{21}} {u_2}^{x_2 + \alpha' y_{12} + m' y_{22}} = v$$

then m' is output as the deciphered results (where $\alpha' = \alpha'_1 \,||\, \alpha'_2$). If not satisfied, then the effect that the received ciphertext is rejected is output as the decipher results.

Further, as recited in independent claim 24, the present invention as described, for example, on page 13, line 6 to page 15, line 18 of the present application, is directed to a public-key cryptographic method implemented in a computer system. The method includes a key generation step of generating a secret-key:

$$\bullet\ x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p,\ d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p,\ d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p,\ h = g_1^{z} \bmod p,$
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$

The method also includes a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for a plaintext m ($|m| = k_3$ where $|x|$ is the number of digits of x), and calculating:

$$\tilde{m} = \alpha || K$$

The ciphertext generation and transmission step also includes selecting a random number rεZq, calculating:

$$u_1 = g_1^{r} \bmod p, \quad u_2 = g_2^{r} \bmod p, \quad e = \tilde{m}\, h^{r} \bmod p, \quad v = g_1^{\alpha_1} c^{r} d_1^{\alpha r} d_2^{mr} \bmod p$$

and transmitting (u_1, u_2, e, v) as a ciphertext. The method also includes a

ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|m'| = k_3$) which satisfy:

$$\alpha'_1 || \alpha'_2 || m' = e/{u_1}^z \bmod p$$

If the following is satisfied:

$${g_1}^{\alpha'_1} {u_1}^{x_1 + \alpha' y_{11} + m' y_{21}} {u_2}^{x_2 + \alpha' y_{12} + m' y_{22}} \equiv v \pmod p$$

then m' is output as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$). If not satisfied, then the effect that the received ciphertext is rejected is output as the decipher results.

Furthermore, as recited in independent claim 28, the present invention as described, for example, on page 15, line 20 to page 19, line 6 of the present application, is directed to a cryptographic communication method implemented in a computer system. The method includes a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1} {g_2}^{x_2}$, $d_1 = {g_1}^{y_{11}} {g_2}^{y_{12}}$, $d_2 = {g_1}^{y_{21}} {g_2}^{y_{22}}$, $h = {g_1}^z$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- E : symmetric encipher function

where the group G is a partial group of the group G', and X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1||\alpha_2 < q \qquad (\forall\alpha_1 \in X_1,\ \forall\alpha_2 \in X_2)$$

M is a key space. The method also includes a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Zq$ for key data K (K ϵ M), calculating:

$$u_1 = {g_1}^r, \quad u_2 = {g_2}^r, \quad e = \pi(\alpha_1, \alpha_2, K)h^r, \quad v = {g_1}^{\alpha_1} c^r {d_1}^{\alpha r} {d_2}^{Kr}$$

where $\alpha = \alpha_1 \,||\, \alpha_2$, generating a ciphertext C of transmission data m by:

$$C = E_K(m)$$

by using a symmetric cryptographic function E and key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext. The method also includes a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, K' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, K'ϵM) which satisfy:

$$\pi(\alpha'_1||\alpha'_2||K') = e/{u_1}^z$$

If the following is satisfied (where $\alpha' = \alpha'_1 \,||\, \alpha'_2$):

$${g_1}^{\alpha'_1} {u_1}^{x_1+\alpha' y_{11}+K' y_{21}} {u_2}^{x_2+\alpha' y_{12}+K' y_{22}} = v$$

a decipher process is executed by:

$$m = D_{K'}(C)$$

The deciphered results are output. If not satisfied, the effect that the received ciphertext is rejected are output as the decipher results.

Yet even further, as recited in independent claim 30, the present invention as described, for example, on page 19, line 6 to page 22, line 14 of the present application, is directed to a cryptographic communication method implemented in a computer system. The method includes a key generation step of generating a secret-key:

$$\bullet\ x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1{}^{x_1} g_2{}^{x_2} \bmod p,\ d_1 = g_1{}^{y_{11}} g_2{}^{y_{12}} \bmod p,\ d_2 = g_1{}^{y_{21}} g_2{}^{y_{22}} \bmod p,\ h = g_1{}^{z} \bmod p,$
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$
- E : symmetric encipher function

The method also includes a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for key data K ($|K| = k_3$ where $|x|$ is the number of digits of x), calculating:

$$\tilde{m} = \alpha || K$$

The ciphertext generation and transmission step also includes selecting a random number $r \epsilon Z_q$, calculating:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad e = \tilde{m}\, h^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d_1{}^{\alpha r} d_2{}^{Kr} \bmod p$$

and generating a ciphertext C of transmission data by:

$$C = E_K(m)$$

by using a (symmetric) cryptographic function E and the key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext. The method also includes a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, K' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|K'| = k_3$) which satisfy:

$$\alpha'_1 || \alpha'_2 || K' = e/{u_1}^z \bmod p$$

If the following is satisfied (where $\alpha' = \alpha'_1 \,||\, \alpha'_2$):

$${g_1}^{\alpha'_1} {u_1}^{x_1+\alpha' y_{11}+K' y_{21}} {u_2}^{x_2+\alpha' y_{12}+K' y_{22}} \equiv v \pmod p$$

a decipher process is executed by:

$$m = D_{K'}(C)$$

The deciphered results are output. If not satisfied, the effect that the received ciphertext is rejected is output as the decipher results.

Still further, as recited in independent claim 35, the present invention as described, for example, on page 22, line16 to page 25, line18 of the present application, is directed to a cryptographic communication method implemented in a computer system. The method includes a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = g_1{}^{x_1} g_2{}^{x_2}$, $d = g_1{}^{y_1} g_2{}^{y_2}$, $h = g_1{}^{z}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow \mathrm{Dom}(E)$: one-to-one mapping
  (Dom(E) is the domain of the function E)
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- H : hash function
- E : symmetric encipher function

where the group G is a partial group of the group G', and X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

The method also includes a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Zq$, calculating:

$$u_1 = g_1{}^{r}, \quad u_2 = g_2{}^{r}, \quad v = g_1{}^{\alpha_1} c^{r} d^{\alpha r}, \quad K = H(h^{r})$$

where $\alpha = \alpha_1 || \alpha_2$, generating a ciphertext C of transmission data m by

$$C = E_K(\pi(\alpha_1, \alpha_2, m))$$

by using a (symmetric) cryptographic function E, and transmitting (u_1, u_2, v, C) as the ciphertext. The method also includes a ciphertext reception and decipher step of calculating:

$$K' = H(u_1{}^{z})$$

by using the secret key, calculating from the received ciphertext, α'_1, α'_2 (where $\alpha'_1 \epsilon X_1$ $\alpha'_2 \epsilon X_2$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = D_{K'}(C)$$

If the following is satisfied (where $\alpha' = \alpha'_1 \,||\, \alpha'_2$):

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} = v,$$

then m' is output as the deciphered results. If not satisfied, the effect that the received ciphertext is rejected is output as the decipher results.

Furthermore, as recited in independent claim 36, the present invention as described, for example, on page 25, line 20 to page 28, line 9 of the present application, is directed to a cryptographic communication method in a computer system. The method includes a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1{}^{x_1} g_2{}^{x_2} \bmod p$, $d = g_1{}^{y_1} g_2{}^{y_2} \bmod p$, $h = g_1{}^{z} \bmod p$,
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$
- H : hash function
- E : symmetric encipher function (the domain of E is all positive integers)

The method also includes a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where ($|x|$ is the number of digits of x), selecting a random number $r \epsilon Z_q$, calculating:

$$u_1 = g_1{}^{r} \bmod p, \quad u_2 = g_2{}^{r} \bmod p, \quad v = g_1{}^{\alpha_1} c^{r} d^{\alpha r} \bmod p, \quad K = H(h^{r} \bmod p)$$

and transmitting the ciphertext (u_1, u_2, v, C). the ciphertext generation and transmission step also includes generating a ciphertext C of transmission data m by:

$$C = E_K(\alpha_1||\alpha_2||m)$$

by using a (symmetric) cryptographic function, and transmitting (u_1, u_2, v, C) as the ciphertext. The method further includes a ciphertext reception and decipher step of calculating:

$$K' = H({u_1}^z \bmod p)$$

by using the secret key, and calculating from the received ciphertext, α'_1, α'_2 ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$) which satisfy:

$$\alpha'_1||\alpha'_2||m' = D_{K'}(C)$$

If the following is satisfied:

$${g_1}^{\alpha'_1}{u_1}^{x_1+\alpha' y_1}{u_2}^{x_2+\alpha' y_2} \equiv v \pmod p$$

then m' is output as the deciphered results (where $\alpha' = \alpha'_1 \,||\, \alpha'_2$). If not satisfied, the effect that the received ciphertext is rejected is output as the decipher results.

Yet even further, as recited in independent claim 40, the present invention as described, for example, on page 28, line 11 to page 31, line 5 of the present application, is directed to a cryptographic communication method implemented in a computer system. The method includes a key generation

step of generating a secret-key:

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (asymmetric cryptography) decipher key

and a public-key:

- G : finite (multiplicative) group
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow \mathrm{Dom}(E)$: one-to-one mapping (Dom(E) is the domain of the function E)
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- $E_{pk}(\cdot)$: (asymmetric cryptography) encipher function

where the group G is a partial group of the group G', and X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

where M is a plaintext space. The method also includes a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Zq$, calculating:

$$u_1 = g_1^{r}, \quad u_2 = g_2^{r}, \quad v = g_1^{\alpha_1} c^{r} d^{\alpha r}$$

where $\alpha = \alpha_1 || \alpha_2$, generating a ciphertext C of transmission data m by:

$$e = E_{pk}(\pi(\alpha_1, \alpha_2, m))$$

by using an (asymmetric) cryptographic function E_{pk}, and transmitting (u_1, u_2,

e, v) as the ciphertext. The method also includes a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, m' ϵ M) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = D_{sk}(e)$$

If the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} = v$$

where:

$$\alpha' = \alpha'_1 || \alpha'_2$$

then m' is output as the deciphered results. If not satisfied, the effect that the received ciphertext is rejected is output as the decipher results.

Still even further, as recited in independent claim 41, the present invention as described, for example, on page 31, line 7 to page 33, line 23 of the present application, is directed to a cryptographic communication method implemented in a computer system. The method includes a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (asymmetric cryptography) decipher key

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1{}^{x_1} g_2{}^{x_2} \bmod p$, $d = g_1{}^{y_1} g_2{}^{y_2} \bmod p$,
- k_1, k_2 : positive constant $(10^{k_1+k_2} < q)$
- $E_{pk}(\cdot)$: (asymmetric cryptography) encipher function (the domain is all positive integers)

The method also includes a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where $|x|$ is the number of digits of x), selecting a random number $r \epsilon Zq$, calculating:

$$u_1 = {g_1}^r \bmod p, \quad u_2 = {g_2}^r \bmod p, \quad v = {g_1}^{\alpha_1} c^r {d^{\alpha r}} \bmod p$$

The ciphertext generation and transmission step also includes generating a ciphertext C of transmission data m (positive integer) by:

$$e = E_{pk}(\alpha_1 || \alpha_2 || m)$$

by using the secret key, and transmitting (u_1, u_2, e, v) as the ciphertext. The method also includes a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, m' is a positive integer) which satisfy:

$$\alpha'_1 || \alpha'_2 || m' = D_{sk}(e)$$

If the following is satisfied:

$${g_1}^{\alpha'_1} {u_1}^{x_1 + \alpha' y_1} {u_2}^{x_2 + \alpha' y_2} \equiv v \pmod p,$$

where:

$$\alpha' = \alpha'_1 || \alpha'_2$$

then m' is output as the deciphered results. If not satisfied, then the effect that the received ciphertext is rejected is output as the decipher results.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 25-27, 29, 31-34, 37-39 and 42-44 are indefinite under 35 USC §112, second paragraph;

Whether claims 23-44 are directed to statutory subject matter as required by 35 USC §101; and

Whether claims 23-44 are obvious over Cramer under 35 USC §103(a).

VII. ARGUMENT

A. 35 USC §112, second paragraph rejection of claim 25-27, 29, 31-34, 37-39 and 42-44

Each of claims 25-27, 29, 31-34, 37-39 and 42-44 are definite and fully comply with the requirements of 35 USC §112, second paragraph. Therefore, reconsideration and withdrawal of the 35 USC §112, second paragraph rejection of claims 25-27, 29, 31-34, 37-39 and 42-44 are respectfully requested.

B. 35 USC §101 rejection of claims 23-44

Each of claims 23-44 is directed to a practical application, namely the encrypting and decrypting of communications in a computer system which implements a public-key or communication cryptographic method. Thus, the claims are directed to a "process" implemented by a "machine" as permitted under 35 USC §101. Therefore, reconsideration and withdrawal of this rejection is respectfully requested.

C. 35 USC §103(a) rejection of claims 23-44

The above described features of the present invention as clearly recited in claims 23-44 are not taught or suggested by any of the references of record, particularly Cramer, whether taken individually or in combination with any of the other references of record.

Cramer teaches a scheme that improves the security of encrypted data or information by using a practical public cryptosystem that is able to resist adaptive attacks. According to Cramer, the scheme does not leak any information of the secret of the used key by generating an extended private key and public key. As per Cramer, a message m, also referred to as plaintext, can be encrypted to obtain a cipher text t by using the public key. This cipher text t can be transmitted over an insecure channel such as the Internet so that only a recipient with the right private key is able to decrypt the cipher text t.

The proof of security according to the system taught by Cramer is based on standard assumptions which are the hardness of the Diffie-Hellman decision problem (DDH problem), wherein the DDH problem is very hard to solve due to the large calculation volume; and the collision intractability of the hash function, which is equivalent to the existence of universal one-way functions.

Cramer employs a hash function in the encryption algorithm as described in col. 7, line 50 to col. 8, line 21 and col. 11, line 60 to col. 12, line 34 thereof. Cramer also discloses a particular encryption method using a hash function and the hash value in claims 11 and 12 thereof.

The proof of security of the present invention as described, for example, on page 4, line 26 through page 7, line 4 of the present application relates to a security system which is also based on an assumption of the hardness of the Diffie-Heilman decision problem. However, the proof security of the present invention, as recited in independent claims 23, 24, 28, 30, 40, and 41, is not based on the above described assumption regarding the collision intractability of the hash function through which the existence of the universal one-way functions are provided. In the present invention, as recited in independent claims 23, 24, 28, 30, 40, and 41, a hash function and a hash value are not used in the encryption process.

As is well known, various cryptographic schemes are based on various assumptions. However, such assumptions are not always realistic. The collision intractability of the hash function has not yet been verified (see page 3, line 27 to page 4, line 24 of the present application). Therefore, contrary to Cramer, the present invention, as recited in independent claims 23, 24, 28, 30, 40, and 41, does not rely on the unverified assumption of the collision intractability of the hash function for encryption and as such is directed to an encryption process entirely different from Cramer.

Thus, as is quite clear from the above, the present invention, as recited in independent claims 23, 24, 28, 30, 40, and 41, is quite different from Cramer, particularly with regard to the assumptions based upon. According to the present invention, as recited in independent claims 23, 24, 28, 30, 40, and 41, hash functions and values are not used in the

encryption process thereof. Therefore, the features of the present invention as recited in the claims are not taught or suggested by Cramer whether taken individually or in combination with any of the other references of record.

Further, Cramer does not assume the random oracle model but assumes a universal one way hash function contrary to that of the present invention. The universal one way hash function is an algorithm which can prove the security. However, it is an ideal function and it is actually replaced with a practical hash function such as SHA-1. This replacement makes the proof of the security insecure. This is an inherent problem of Cramer. Attention is directed to the article entitled "Random Oracle", which was filed in an Information Disclosure Statement on even date herewith. This phenomenon is well-known as discussed on page 5, lines 19 and 21 of the present application and as discussed column 5, lines 44 to 47 of Cramer. Cramer refers to this phenomenon as "collision resistant hash functions."

The present invention, as recited in independent claims 23, 24, 28, 30, 40, and 41, does not assume the universal one way hash function and provides an encryption scheme more efficient than Cramer.

In Cramer, the public key includes one element “d” as shown in Fig. 2 and as discussed at column 7, lines 26 to 39 thereof. The element “d” as per Cramer relates to the two elements y1 and y2 of the private key. Cramer does not disclose the detailed structure of the public key, as recited in independent claims 23, 24, 28, and 30. Further, the Examiner

does not indicate the relation of each element of the public key between Cramer and the present invention.

In the present invention, as recited in independent claims 23, 24, 28, and 30, the public key includes two elements "d1" and "d2". The "d1" and "d2" of the present invention respectively relate to the two elements y11 and y12, and y21 and y22 of the private key. Each of independent claims 23, 24, 28 and 30 of the present application includes "d1" and "d2" in the public key at the key generation step. The ciphertext generating step of the present invention, as recited in independent claims 23, 24, 28, and 30, uses the two elements "d1" and "d2", and the ciphertext decipher step of the present invention, as recited in independent claims 23, 24, 28, and 30, uses the four elements of y11, y12, y21 and y22 of the private key.

A particularity exists in the field of cryptosystem algorithm. Even if the security and the computation amount are largely improved in the cryptosystem, the difference between the conventional algorithm and the new algorithm appears to be very small when they are expressed by the mathematical expressions. If the difference on the mathematical expressions is small, the theory to make the difference is not small and the effect derived from the difference is large.

The features of the present invention, as recited in independent claims 23, 24, 28, and 30, include two d parameters (i.e., "d1" and "d2"). Adding more parameters to the key generation steps will greatly increase the computation amount. In the cryptosystem in Cramer, the computation amount is large (see, e.g., *A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack* ("Cramer treatise")), which is

written by the inventors of Cramer patent and appears to show the detailed algorithm of the Cramer patent (U.S. Patent No. 6,697,488). The variables used in the expressions of the Cramer treatise and the Cramer patent are identical.

Assume the message m is encrypted as follows in Cramer:

$u_1=(g_1)^r \bmod p$

$u_2=(g_2)^r \bmod p$

$e=mh^r \bmod p$,

$v=c^r d^{rZ}$, where $z=H(u_1, u_2, e)$ and H is a hash function.

The variables p and q are prime numbers satisfying q/p-1, which means that p-1 is divisible by q. The order of g_1 and g_2 is q and p is around 1024 bits.

In the hash-free variant (page 15, section 5.3 of Cramer treatise), the following replacement is performed:

At first, (u_1, u_2, e) is replaced with $(a_1,\ldots,a_k)$, where $0 < a_i < q$.

Further, $d_i=(g_1)^{y\_\{i1\}}(g_2)^{y\_\{i2\}} \bmod p$, where $0<i<k$ is calculated and made open.

In the above-mentioned encryption, the calculation of v is replaced with:

$$v=c^r(d_1)^{ra\_1}\ldots(d_k)^{ra\_k}$$

As mentioned above, the number of d_1 is determined by the value of k. To improve the efficiency of the encryption system, i.e. to reduce the calculation amount of v, it is preferable that the number of d (the value of k) is small.

In the Cramer patent, when p-1 = 2q, k can be 3. Since the value of q is large in this case, the calculation amount of u_1 and u_2 will be large, which is

a problem of Cramer. Conversely, when the value of q is set around 160 bits, k will be more than 20 and the calculation amount of v becomes large.

The present invention provides an encryption system in which the value of k is kept small (k is 2) and the calculation amount of u_1 and u_2 is also kept small. The number of plural d_i is more than 3 in Cramer while the number of d_i is 2 in the present invention. This difference contributes the computation amount reduction. Accordingly, the present invention is different from Cramer in at least the number of d_i, which is not a simple parameter addition.

Thus, the present invention as recited in the claims differs substantially from Cramer in that Cramer fails to teach or suggest the key generation step, ciphertext generation step and ciphertext decipher step as recited in the claims.

i. Independent Claim 23

One feature of the present invention, as recited in independent claim 23, includes a key generation step of generating a secret key and a public key. The secret key includes x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, and z. The public key includes elements d_1 and d_2. The element d_1 relates to the elements y_{11} and y_{12} of the secret key, and the element d_2 relates to the elements y_{21} and y_{22} of the secret key. Cramer does not disclose this feature. To support the assertion that Cramer teaches a key generation step of generating a secret key and a public key, in the manner claimed, the Examiner cites column 7, lines 1-67. However, neither the cited text, nor any other portion of Cramer, teaches the claimed feature.

For example, as described in column 7, lines 11-19, Cramer discloses where a first exponent-number x_1, a second exponent-number x_2, a third exponent-number Z, a fourth exponent-number y_1, and a fifth exponent-number y_2, are chosen at random for the private key. As such, Cramer discloses the use of elements y_1 and y_2. To the contrary, in the present invention, the secret key includes y_{11}, y_{12}, y_{21}, y_{22}. Cramer does not teach or suggest the additional elements of the claimed invention.

By way of further example, as described in column 7, lines 25-27, Cramer discloses where the public key is "represented by the numbers g_1, g_2, c, d, and h." Accordingly, Cramer only discloses one element d, whereas the present invention discloses where the public key includes both an element d_1 and an element d_2. As such, Cramer fails to teach or suggest where the public key includes both elements d_1 and d_2, as in the present invention.

On page 9 of the Office Action (see, e.g., the last paragraph) mailed on February 7, 2007, and in the Advisory Action mailed on September 21, 2006, the Examiner appears to concede that Cramer does not teach where the secret key includes all of the elements y_{11}, y_{12}, y_{21}, y_{22} of the present invention. However, the Examiner contends that "it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate the secret key by modifying Cramer's generating step." The Examiner further contends that "One of ordinary skill in the art would have been motivated to do so to increase the security of the cryptographic scheme", citing column 3, lines 1-67 and column 4, lines 1-67 of Cramer.

However, the cited text does not provide the motivation relied upon by the Examiner to modify Cramer's generating step. Instead, the Examiner has

resorted to hindsight, based upon Applicants' disclosure, rather than relying upon facts gleaned from the prior art. Therefore, the Examiner has relied upon impermissible hindsight to conclude that it would be obvious to modify Cramer to obtain the present invention.

Furthermore, as described in column 9, lines 65-67, Cramer describes where, in order to achieve security against lunch-time attacks, "one can simplify the above-described basic scheme" by omitting d, y_1 and y_2. As such, Cramer teaches away from adding additional elements, so as to include both elements d_1 and d_2 in the public key, and each of elements y_{11}, y_{12}, y_{21}, y_{22} in the secret key. Therefore, contrary to the Examiner's assertions, it would not be obvious to modify Cramer to add the additional elements, so as to achieve the present invention.

Therefore, Cramer fails to teach or suggest "a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d_1 = g_1^{y_{11}} g_2^{y_{12}}$, $d_2 = g_1^{y_{21}} g_2^{y_{22}}$, $h = g_1^{z}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

where M is a plaintext space" as recited in independent claim 23.

Another feature of the present invention, as recited in independent claim 23, includes a ciphertext generation and transmission step of selecting random numbers for a plaintext m, calculating u_1, u_2, e, and v, where:

$$e = \pi\,(\alpha_1, \alpha_2, m)\, h_r \quad \text{, and} \quad v = g_1^{\alpha 1}\, c^r\, d_1^{ar}\, d_2^{mr} \quad .$$

Cramer does not disclose this feature. To support the assertion that Cramer teaches a ciphertext generation and transmission step, in the manner claimed, the Examiner cites column 7, lines 1-67 and column 8, lines 1-67. Neither the cited text, nor any other portion of Cramer, teaches the claimed feature.

For example, as described in column 7, line 56 to column 8, line 21, Cramer discloses where the encryption means computes a first universal cipher-number u_1, an encryption cipher-number e, a hash-value a, and a verification cipher-number v. The verification cipher-number v is based on the first group-number c, the third group-number d, the hash-value a, and the single exponent-number r. The present invention, as recited in claim 23, does not rely upon a hash function, and thus, does not use a hash-value a. In this way, for example, Cramer is clearly different from the claimed invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r\, d^a$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{\alpha 1}\, c^r\, d_1^{\alpha r}\, d_2^{mr}$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

By way of further example, as shown in column 8, line 5, Cramer discloses where the encryption cipher-number e is calculated according to the following formula: $e = h^r\, m$. This is quite different from the present invention,

where $e = \pi(\alpha_1, \alpha_2, m)\, h_r$, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Zq$ for a plaintext m ($m \epsilon M$), calculating:

$$u_1 = g_1{}^r, \quad u_2 = g_2{}^r, \quad e = \pi(\alpha_1, \alpha_2, m)h^r, \quad v = g_1{}^{\alpha_1} c^r d_1{}^{\alpha r} d_2{}^{mr}$$

where $\alpha = \alpha_1 \,||\, \alpha_2$, and transmitting ($u_1$, u_2, e, v) as a ciphertext" as recited in independent claim 23.

Yet another feature of the present invention, as recited in independent claim 23, includes a ciphertext reception and decipher step. This step includes a condition, such that a step is performed of outputting m' as the deciphered results, if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+m' y_{21}} u_2{}^{x_2+\alpha' y_{12}+m' y_{22}} = v$$

If the above condition is not satisfied, then a step is performed of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature. To support the assertion that Cramer teaches this feature, the Examiner cites columns 9-11. However, neither the cited text, nor any other portions of Cramer, teach or suggest the claimed features.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1{}^{x1+y1a}\, u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not

provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, m' ϵ M) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = e/{u_1}^z$$

and if the following is satisfied:

$${g_1}^{\alpha'_1} {u_1}^{x_1+\alpha' y_{11}+m' y_{21}} {u_2}^{x_2+\alpha' y_{12}+m' y_{22}} = v$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 23.

ii. Independent Claim 24

One feature of the present invention, as recited in independent claim 24, includes a key generation step of generating a secret key and a public key. The secret key includes x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, and z. The public key includes elements d_1 and d_2, and the elements c, d_1, d_2, and h are calculated using modulo arithmetic. The element d_1 relates to the elements y_{11} and y_{12} of the secret key, and the element d_2 relates to the elements y_{21} and y_{22} of the secret key. Cramer does not disclose this feature. To support the assertion that Cramer teaches a key generation step of generating a secret key and a public key, in the manner claimed, the Examiner cites column 7, lines 1-67.

However, neither the cited text, nor any other portion of Cramer, teaches the claimed feature.

For example, as previously discussed, column 7, lines 11-19 of Cramer describes where a first exponent-number x_1, a second exponent-number x_2, a third exponent-number Z, a fourth exponent-number y_1, and a fifth exponent-number y_2, are chosen at random for the private key. As such, Cramer discloses the use of elements y_1 and y_2. To the contrary, in the present invention, the secret key includes y_{11}, y_{12}, y_{21}, y_{22}. Cramer does not teach or suggest the additional elements of the claimed invention.

By way of further example, as previously discussed, column 7, lines 25-27 of Cramer describes where the public key is "represented by the numbers g_1, g_2, c, d, and h." Accordingly, Cramer only discloses one element d, whereas the present invention discloses where the public key includes both an element d_1 and an element d_2. As such, Cramer fails to teach or suggest where the public key includes both elements d_1 and d_2, as in the present invention.

As previously discussed, and contrary to the Examiner's assertions, Cramer does not provide the motivation relied upon by the Examiner to modify Cramer's generating step. Instead, the Examiner has resorted to hindsight, based upon Applicants' disclosure, rather than relying upon facts gleaned from the prior art. Therefore, the Examiner has relied upon impermissible hindsight to conclude that it would be obvious to modify Cramer to obtain the present invention.

Furthermore, as previously discussed, Cramer teaches away from adding additional elements to obtain the present invention. As described in

column 9, lines 65-67, Cramer describes where, in order to achieve security against lunch-time attacks, "one can simplify the above-described basic scheme" by omitting d, y_1 and y_2. As such, Cramer teaches away from adding additional elements, so as to include both elements d_1 and d_2 in the public key, and each of elements y_{11}, y_{12}, y_{21}, y_{22} in the secret key. Therefore, contrary to the Examiner's assertions, it would not be obvious to modify Cramer to add the additional elements, so as to achieve the present invention.

By way of even further example, column 7, lines 25-27 of Cramer describes where the public key is "represented by the numbers g_1, g_2, c, d, and h", and column 7, line 25 shows the calculations used to derive the numbers c, d and h. As shown, Cramer does not disclose the use of modulo arithmetic in the equations used to calculate c, d and h. This is quite different from the present invention, where the step of generating a public key includes the elements c, d_1, d_2, and h, which are calculated using modulo arithmetic. Accordingly, Cramer does not teach generating a public key in the manner claimed, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1^{x_1} g_2^{x_2} \bmod p$, $d_1 = g_1^{y_{11}} g_2^{y_{12}} \bmod p$, $d_2 = g_1^{y_{21}} g_2^{y_{22}} \bmod p$, $h = g_1^{z} \bmod p$,
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$

" as recited in independent claim 24.

Another feature of the present invention, as recited in independent claim 24, includes a ciphertext generation and transmission step of selecting random numbers for a plaintext m, calculating u_1, u_2, e, and v, where:

$$u_1 = g_1^{r} \bmod p, \quad u_2 = g_2^{r} \bmod p, \quad e = \tilde{m}\, h^{r} \bmod p, \quad v = g_1^{\alpha_1} c^{r} d_1^{\alpha r} d_2^{mr} \bmod p$$

Cramer does not disclose this feature. To support the assertion that Cramer teaches a ciphertext generation and transmission step, in the manner claimed, the Examiner cites column 8, lines 1-67. Neither the cited text, nor any other portions of Cramer, teaches the claimed feature.

For example, as described in column 7, line 56 to column 8, line 21, Cramer discloses where the encryption means computes a first universal cipher-number u_1, an encryption cipher-number e, a hash-value a, and a verification cipher-number v. The verification cipher-number v is based on the first group-number c, the third group-number d, the hash-value a, and the single exponent-number r. The present invention, as recited in claim 24, does not rely upon a hash function, and thus, does not use a hash-value a. In this way, for example, Cramer is clearly different from the claimed invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{ra}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1} c^r d_1^{ar} d_2^{mr} \bmod p$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

By way of further example, as shown in column 8, line 5, Cramer discloses the formulas used for calculating u_1, u_2, e, and v. As shown, Cramer does not disclose the use of modulo arithmetic in the equations used to calculate u_1, u_2, e, and v. This is quite different from the present invention, where the step of generating a public key includes where the elements u_1, u_2, e, and v are calculated using modulo arithmetic. Accordingly, Cramer does not teach generating a public key in the manner claimed, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for a plaintext m ($|m| = k_3$ where $|x|$ is the number of digits of x), calculating:

$$\tilde{m} = \alpha || K$$

selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1^{\,r} \bmod p, \quad u_2 = g_2^{\,r} \bmod p, \quad e = \tilde{m}\, h^r \bmod p, \quad v = g_1^{\,\alpha_1} c^r d_1^{\,\alpha r} d_2^{\,mr} \bmod p$$

and transmitting (u_1, u_2, e, v) as a ciphertext" as recited in independent claim 24.

Yet another feature of the present invention, as recited in independent claim 24, includes a ciphertext reception and decipher step. This step includes a condition, such that a step is performed of outputting m' as the deciphered results, if the following is satisfied:

$$g_1^{\,\alpha'_1} u_1^{\,x_1+\alpha' y_{11}+m' y_{21}} u_2^{\,x_2+\alpha' y_{12}+m' y_{22}} \equiv v \pmod p$$

If the above condition is not satisfied, then a step is performed of outputting, as the decipher results, the effect that the received ciphertext is rejected. Cramer does not disclose this feature. To support the assertion that Cramer teaches this feature, the Examiner cites columns 9-11. However, neither the cited text, nor any other portions of Cramer, teach or suggest the claimed features.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|m'| = k_3$) which satisfy:

$$\alpha'_1||\alpha'_2||m' = e/{u_1}^z \bmod p$$

and if the following is satisfied:

$${g_1}^{\alpha'_1}{u_1}^{x_1+\alpha' y_{11}+m' y_{21}}{u_2}^{x_2+\alpha' y_{12}+m' y_{22}} \equiv v \pmod p$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 24.

iii. Independent Claim 28

One feature of the present invention, as recited in independent claim 28, includes a key generation step of generating a secret key and a public key. The secret key includes x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, and z. The public key includes elements d_1 and d_2. The element d_1 relates to the elements y_{11} and y_{12} of the secret key, and the element d_2 relates to the elements y_{21} and y_{22} of the secret key. Cramer does not disclose this feature. To support the assertion that Cramer teaches a key generation step of generating a secret key and a public key, in the manner claimed, the Examiner cites column 7, lines 1-67. However, neither the cited text, nor any other portion of Cramer, teaches the claimed feature.

For example, as previously discussed, column 7, lines 11-19 of Cramer describes where a first exponent-number x_1, a second exponent-number x_2, a third exponent-number Z, a fourth exponent-number y_1, and a fifth exponent-number y_2, are chosen at random for the private key. As such, Cramer discloses the use of elements y_1 and y_2. To the contrary, in the present invention, the secret key includes y_{11}, y_{12}, y_{21}, y_{22}. Cramer does not teach or suggest the additional elements of the claimed invention.

By way of further example, as previously discussed, column 7, lines 25-27 of Cramer describes where the public key is "represented by the numbers g_1, g_2, c, d, and h." Accordingly, Cramer only discloses one element d, whereas the present invention discloses where the public key includes both an element d_1 and an element d_2. As such, Cramer fails to teach or suggest where the public key includes both elements d_1 and d_2, as in the present invention.

As previously discussed, and contrary to the Examiner's assertions, Cramer does not provide the motivation relied upon by the Examiner to modify Cramer's generating step. Instead, the Examiner has resorted to hindsight, based upon Applicants' disclosure, rather than relying upon facts gleaned from the prior art. Therefore, the Examiner has relied upon impermissible hindsight to conclude that it would be obvious to modify Cramer to obtain the present invention.

Furthermore, as previously discussed, Cramer teaches away from adding additional elements to obtain the present invention. As described in column 9, lines 65-67, Cramer describes where, in order to achieve security against lunch-time attacks, "one can simplify the above-described basic scheme" by omitting d, y_1 and y_2. As such, Cramer teaches away from adding additional elements, so as to include both elements d_1 and d_2 in the public key, and each of elements y_{11}, y_{12}, y_{21}, y_{22} in the secret key. Therefore, contrary to the Examiner's assertions, it would not be obvious to modify Cramer to add the additional elements, so as to achieve the present invention.

Therefore, Cramer fails to teach or suggest "a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d_1 = g_1^{y_{11}} g_2^{y_{12}}$, $d_2 = g_1^{y_{21}} g_2^{y_{22}}$, $h = g_1^{z}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- E : symmetric encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

where M is a key space" as recited in independent claim 28 of the present invention.

Another feature of the present invention, as recited in independent claim 28, includes a ciphertext generation and transmission step of selecting random numbers for key data K, calculating u_1, u_2, e, and v, where:

$$e = \pi(\alpha_1, \alpha_2, K)\, h_r \quad \text{, and} \quad v = g_1^{a1}\, c^r\, d_1^{ar}\, d_2^{Kr} \quad .$$

Cramer does not disclose this feature. To support the assertion that Cramer teaches a ciphertext generation and transmission step, in the manner claimed, the Examiner cites column 7, lines 1-67 and column 8, lines 1-67. Neither the cited text, nor any other portion of Cramer, teaches the claimed feature.

For example, as described in column 7, line 56 to column 8, line 21, Cramer discloses where the encryption means computes a first universal cipher-number u_1, an encryption cipher-number e, a hash-value a, and a verification cipher-number v. The verification cipher-number v is based on the first group-number c, the third group-number d, the hash-value a, and the single exponent-number r. The present invention, as recited in claim 28, does not rely upon a hash function, and thus, does not use a hash-value a. In this way, for example, Cramer is clearly different from the claimed invention.

Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{ra}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1} c^r d_1^{ar} d_2^{Kr}$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

By way of further example, as shown in column 8, line 5, Cramer discloses where the encryption cipher-number e is calculated according to the following formula: $e = h^r m$. This is quite different from the present invention, where $e = \pi (\alpha_1, \alpha_2, K) h_r$, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Zq$ for key data K ($K \epsilon M$), calculating:

$$u_1 = g_1{}^r, \quad u_2 = g_2{}^r, \quad e = \pi(\alpha_1, \alpha_2, K)h^r, \quad v = g_1{}^{\alpha_1} c^r d_1{}^{\alpha r} d_2{}^{Kr}$$

where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by:

$$C = E_K(m)$$

by using a (symmetric cryptographic function E and key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext" as recited in independent claim 28.

Yet another feature of the present invention, as recited in independent claim 28, includes a ciphertext reception and decipher step. This step

includes a condition, such that a step is performed of executing a decipher process, if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+K' y_{21}} u_2{}^{x_2+\alpha' y_{12}+K' y_{22}} = v$$

If the above condition is not satisfied, then a step is performed of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature. To support the assertion that Cramer teaches this feature, the Examiner cites columns 9-11. However, neither the cited text, nor any other portions of Cramer, teach or suggest the claimed features.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1{}^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, K' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, K' ϵ M) which satisfy:

$$\pi(\alpha'_1 || \alpha'_2 || K') = e/u_1{}^z$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+K' y_{21}} u_2{}^{x_2+\alpha' y_{12}+K' y_{22}} = v$$

where $\alpha' = \alpha'_1 || \alpha'_2$

executing a decipher process by:

$$m = D_{K'}(C)$$

outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 28.

iv. Independent Claim 30

One feature of the present invention, as recited in independent claim 30, includes a key generation step of generating a secret key and a public key. The secret key includes x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, and z. The public key includes elements d_1 and d_2. The element d_1 relates to the elements y_{11} and y_{12} of the secret key, and the element d_2 relates to the elements y_{21} and y_{22} of the secret key. Cramer does not disclose this feature. To support the assertion that Cramer teaches a key generation step of generating a secret key and a public key, in the manner claimed, the Examiner cites column 7, lines 1-67. However, neither the cited text, nor any other portion of Cramer, teaches the claimed feature.

For example, as previously discussed, column 7, lines 11-19 of Cramer describes where a first exponent-number x_1, a second exponent-number x_2, a third exponent-number Z, a fourth exponent-number y_1, and a fifth exponent-number y_2, are chosen at random for the private key. As such, Cramer discloses the use of elements y_1 and y_2. To the contrary, in the present invention, the secret key includes y_{11}, y_{12}, y_{21}, y_{22}. Cramer does not teach or suggest the additional elements of the claimed invention.

By way of further example, as previously discussed, column 7, lines 25-27 of Cramer describes where the public key is "represented by the

numbers g_1, g_2, c, d, and h." Accordingly, Cramer only discloses one element d, whereas the present invention discloses where the public key includes both an element d_1 and an element d_2. As such, Cramer fails to teach or suggest where the public key includes both elements d_1 and d_2, as in the present invention.

As previously discussed, and contrary to the Examiner's assertions, Cramer does not provide the motivation relied upon by the Examiner to modify Cramer's generating step. Instead, the Examiner has resorted to hindsight, based upon Applicants' disclosure, rather than relying upon facts gleaned from the prior art. Therefore, the Examiner has relied upon impermissible hindsight to conclude that it would be obvious to modify Cramer to obtain the present invention.

Furthermore, as previously discussed, Cramer teaches away from adding additional elements to obtain the present invention. As described in column 9, lines 65-67, Cramer describes where, in order to achieve security against lunch-time attacks, "one can simplify the above-described basic scheme" by omitting d, y_1 and y_2. As such, Cramer teaches away from adding additional elements, so as to include both elements d_1 and d_2 in the public key, and each of elements y_{11}, y_{12}, y_{21}, y_{22} in the secret key. Therefore, contrary to the Examiner's assertions, it would not be obvious to modify Cramer to add the additional elements, so as to achieve the present invention.

Therefore, Cramer fails to teach or suggest "<u>a key generation step of generating a secret-key:</u>

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = {g_1}^{x_1} {g_2}^{x_2} \bmod p$, $d_1 = {g_1}^{y_{11}} {g_2}^{y_{12}} \bmod p$, $d_2 = {g_1}^{y_{21}} {g_2}^{y_{22}} \bmod p$, $h = {g_1}^{z} \bmod p$,
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$
- E : symmetric encipher function

" as recited in independent claim 30.

Another feature of the present invention, as recited in independent claim 30, includes a ciphertext generation and transmission step of selecting random numbers for key data K, calculating u_1, u_2, e, and v, where:

$$u_1 = {g_1}^{r} \bmod p, \quad u_2 = {g_2}^{r} \bmod p, \quad e = \widetilde{m}\, h^{r} \bmod p, \quad v = {g_1}^{\alpha_1} c^{r} {d_1}^{\alpha r} {d_2}^{Kr} \bmod p$$

Cramer does not disclose this feature. To support the assertion that Cramer teaches a ciphertext generation and transmission step, in the manner claimed, the Examiner cites columns 7, 8 and 12. However, neither the cited text, nor any other portions of Cramer, teaches the claimed feature.

For example, as described in column 7, line 56 to column 8, line 21, Cramer discloses where the encryption means computes a first universal cipher-number u_1, an encryption cipher-number e, a hash-value a, and a verification cipher-number v. The verification cipher-number v is based on the first group-number c, the third group-number d, the hash-value a, and the single exponent-number r. The present invention, as recited in claim 30, does not rely upon a hash function, and thus, does not use a hash-value a. In this way, for example, Cramer is clearly different from the claimed invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v =$

$c^r\ d^{r_a}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1}\ c^r\ d_1^{ar}\ d_2^{Kr}\ mod\ p$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

By way of further example, as shown in column 8, line 5, Cramer discloses the formulas used for calculating u_1, u_2, e, and v. As shown, Cramer does not disclose the use of modulo arithmetic in the equations used to calculate u_1, u_2, e, and v. This is quite different from the present invention, where the step of generating a public key includes where the elements u_1, u_2, e, and v are calculated using modulo arithmetic. Accordingly, Cramer does not teach generating a public key in the manner claimed, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for key data K ($|K| = k_3$ where $|x|$ is the number of digits of x), calculating:

$$\tilde{m} = \alpha || K$$

selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1^{\,r} \bmod p, \quad u_2 = g_2^{\,r} \bmod p, \quad e = \tilde{m}\, h^r \bmod p, \quad v = g_1^{\,\alpha_1} c^r d_1^{\,\alpha r} d_2^{\,Kr} \bmod p$$

and generating a ciphertext C of transmission data by:

$$C = E_K(m)$$

by using a (symmetric) cryptographic function E and the key data K, and

transmitting (u_1, u_2, e, v, C) as the ciphertext" as recited in independent claim 30.

Yet another feature of the present invention, as recited in independent claim 30, includes a ciphertext reception and decipher step. This step includes a condition, such that a step is performed of executing a decipher process, if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+K' y_{21}} u_2{}^{x_2+\alpha' y_{12}+K' y_{22}} \equiv v \pmod{p}$$

If the above condition is not satisfied, then a step is performed of outputting, as the decipher results, the effect that the received ciphertext is rejected. Cramer does not disclose this feature. To support the assertion that Cramer teaches this feature, the Examiner cites columns 9-11. However, neither the cited text, nor any other portions of Cramer, teach or suggest the claimed features.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1{}^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, K' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|K'| = k_3$) which satisfy:

$$\alpha'_1 || \alpha'_2 || K' = e/u_1{}^z \bmod p$$

and if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_{11}+K' y_{21}} u_2^{x_2+\alpha' y_{12}+K' y_{22}} \equiv v \pmod{p}$$

where $\alpha' = \alpha'_1 \| \alpha'_2$,

executing a decipher process by:

$$m = D_{K'}(C)$$

outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 30.

v. Independent Claim 35

One feature of the present invention, as recited in independent claim 35, includes a ciphertext generation and transmission step of selecting random numbers, calculating u_1, u_2, v, and K, where:

$v = g_1^{a1} c^r d^{ar}$, and $K = H(h^r)$.

Cramer does not disclose this feature. To support the assertion that Cramer teaches a ciphertext generation and transmission step, in the manner claimed, the Examiner cites columns 7 and 8, and column 12, lines 1-35. However, neither the cited text, nor any other portion of Cramer, teaches the claimed feature.

For example, as described in column 7, line 56 to column 8, line 21, Cramer discloses where the encryption means computes a first universal cipher-number u_1, an encryption cipher-number e, a hash-value a, and a verification cipher-number v. The verification cipher-number v is based on the first group-number c, the third group-number d, the hash-value a, and the single exponent-number r. The present invention, as recited in claim 35, does

not rely upon the hash function in the calculation of v. Furthermore, unlike the present invention, Cramer does not rely upon g_1^{a1} in the calculation of v. In this way, for example, Cramer is clearly different from the claimed invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{ra}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1} c^r d^{ar}$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

By way of further example, as shown in column 8, line 5, Cramer does not disclose where the ciphertext generation and transmission step includes the calculation of the element K (i.e., $K = H(h^r)$), as in the present invention. Cramer merely discloses the calculation of the group of elements u_1, u_2, e, a, and v, which does not include the element K, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \in X_1$, $\alpha_2 \in X_2$, $r \in Zq$, calculating:

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad v = g_1^{\alpha_1} c^r d^{\alpha r}, \quad K = H(h^r)$$

where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by

$$C = E_K(\pi(\alpha_1, \alpha_2, m))$$

by using a (symmetric) cryptographic function E; and transmitting (u_1, u_2, v, C) as the ciphertext" as recited in independent claim 35.

Another feature of the present invention, as recited in independent claim 35, includes a ciphertext reception and decipher step. This step includes a condition, such that a step of outputting m' as the deciphered results if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_1} u_2^{x_2+\alpha' y_2} = v,$$

If the above condition is not satisfied, then a step of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature. To support the assertion that Cramer teaches this feature, the Examiner cites columns 9-11. However, neither the cited text nor any other portions of Cramer, teach or suggest the claimed features.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating:

$$K' = H(u_1^{z})$$

by using the secret key, calculating from the received ciphertext, α'_1, α'_2 (where $\alpha'_1 \epsilon X_1$ $\alpha'_2 \epsilon X_2$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = D_{K'}(C)$$

if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_1} u_2^{x_2+\alpha' y_2} = v,$$

where $\alpha' = \alpha'_1 || \alpha'_2$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 35.

vi. Independent Claim 36

One feature of the present invention, as recited in independent claim 36, includes a ciphertext generation and transmission step of selecting random numbers, calculating u_1, u_2, v, and K, where:

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad v = g_1^{\alpha_1} c^r d^{\alpha r} \bmod p, \quad K = H(h^r \bmod p)$$

Cramer does not disclose this feature. To support the assertion that Cramer teaches a ciphertext generation and transmission step, in the manner claimed, the Examiner cites columns 7 and 8, and column 12, lines 1-35. However, neither the cited text, nor any other portion of Cramer, teaches the claimed feature.

For example, as described in column 7, line 56 to column 8, line 21, Cramer discloses where the encryption means computes a first universal cipher-number u_1, an encryption cipher-number e, a hash-value a, and a verification cipher-number v. The verification cipher-number v is based on the first group-number c, the third group-number d, the hash-value a, and the

single exponent-number r. The present invention, as recited in claim 36, does not rely upon the hash function in the calculation of v. Furthermore, unlike the present invention, Cramer does not rely upon g_1^{a1} in the calculation of v. In this way, for example, Cramer is clearly different from the claimed invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{ra}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1} c^r d^{ar} \bmod p$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

By way of further example, as shown in column 8, line 5, Cramer does not disclose where the ciphertext generation and transmission step includes the calculation of the element K (i.e., $K = H(h^r \bmod p)$), as in the present invention. Cramer merely discloses the calculation of the group of elements u_1, u_2, e, a, and v, which does not include the element K, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

By way of even further example, as shown in column 8, line 5, Cramer discloses the formulas used for calculating u_1, u_2, e, and v. As shown, Cramer does not disclose the use of modulo arithmetic in the equations used to calculate u_1, u_2, e, and v. This is quite different from the present invention, where the step of generating a public key includes where the elements u_1, u_2, v, and K are calculated using modulo arithmetic. Accordingly, Cramer does not teach generating a public key in the manner claimed, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where ($|x|$ is the number of digits of x), selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1^r \bmod p, \quad u_2 = g_2^r \bmod p, \quad v = g_1^{\alpha_1} c^r d^{\alpha r} \bmod p, \quad K = H(h^r \bmod p)$$

transmitting the ciphertext (u_1, u_2, v, C); generating a ciphertext C of transmission data m by:

$$C = E_K(\alpha_1 || \alpha_2 || m)$$

by using a (symmetric) cryptographic function, and transmitting (u_1, u_2, v, C) as the ciphertext" as recited in independent claim 36.

Another feature of the present invention, as recited in independent claim 36, includes a ciphertext reception and decipher step. This step includes a condition, such that a step of outputting m' as the deciphered results if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_1} u_2^{x_2+\alpha' y_2} \equiv v \pmod p$$

If the above condition is not satisfied, then a step of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature. To support the assertion that Cramer teaches this feature, the Examiner cites columns 9-11. However, neither the cited text nor any other portions of Cramer teach or suggest the claimed features.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the

same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating:

$$K' = H({u_1}^z \bmod p)$$

by using the secret key, calculating from the received ciphertext, α'_1, α'_2 ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$) which satisfy:

$$\alpha'_1 || \alpha'_2 || m' = D_{K'}(C)$$

and if the following is satisfied:

$${g_1}^{\alpha'_1} {u_1}^{x_1+\alpha' y_1} {u_2}^{x_2+\alpha' y_2} \equiv v \pmod p$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 36.

vii. Independent Claim 40

One feature of the present invention, as recited in independent claim 40, includes a ciphertext generation and transmission step of selecting random numbers, calculating u_1, u_2 and v, where:

$$v = {g_1}^{a1} c^r d^{ar} \quad .$$

Cramer does not disclose this feature. To support the assertion that Cramer teaches a ciphertext generation and transmission step, in the manner claimed, the Examiner cites columns 7 and 8, and column 12, lines 1-35. However, neither the cited text, nor any other portion of Cramer, teaches the claimed feature.

For example, as described in column 7, line 56 to column 8, line 21, Cramer discloses where the encryption means computes a first universal cipher-number u_1, an encryption cipher-number e, a hash-value a, and a verification cipher-number v. The verification cipher-number v is based on the first group-number c, the third group-number d, the hash-value a, and the single exponent-number r. The present invention, as recited in claim 40, does not rely upon the hash function, and thus, does not use a hash-value a. Furthermore, unlike the present invention, Cramer does not rely upon g_1^{a1} in the calculation of v. In this way, for example, Cramer is clearly different from the claimed invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{ra}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1} c^r d^{ar}$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest " a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Zq$, calculating:

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad v = g_1^{\alpha_1} c^r d^{\alpha r}$$

where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by:

$$e = E_{pk}(\pi(\alpha_1, \alpha_2, m))$$

by using an (asymmetric) cryptographic function E_{pk}, and transmitting (u_1, u_2, e, v) as the ciphertext" as recited in independent claim 40.

Another feature of the present invention, as recited in independent claim 40, includes a ciphertext reception and decipher step. This step includes a condition, such that a step of outputting m' as the deciphered results if the following is satisfied:

$$g_1^{\alpha'_1} u_1^{x_1+\alpha' y_1} u_2^{x_2+\alpha' y_2} = v,$$

If the above condition is not satisfied, then a step of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature. To support the assertion that Cramer teaches this feature, the Examiner cites columns 9-11. However, neither the cited text nor any other portions of Cramer teach or suggest the claimed features.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, $m' \epsilon M$) which satisfy:

$$\pi(\alpha_1', \alpha_2', m') = D_{sk}(e)$$

and if the following is satisfied:

$$g_1{}^{\alpha_1'} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} = v$$

where:

$$\alpha' = \alpha_1' || \alpha_2'$$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 40.

vii. Independent Claim 41

One feature of the present invention, as recited in independent claim 41, includes a ciphertext generation and transmission step of selecting random numbers, calculating u_1, u_2 and v, where:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d^{\alpha r} \bmod p$$

Cramer does not disclose this feature. To support the assertion that Cramer teaches a ciphertext generation and transmission step, in the manner claimed, the Examiner cites columns 7 and 8, and column 12, lines 1-35. However, neither the cited text, nor any other portion of Cramer, teaches the claimed feature.

For example, as described in column 7, line 56 to column 8, line 21, Cramer discloses where the encryption means computes a first universal

cipher-number u_1, an encryption cipher-number e, a hash-value a, and a verification cipher-number v. The verification cipher-number v is based on the first group-number c, the third group-number d, the hash-value a, and the single exponent-number r. The present invention, as recited in claim 41, does not rely upon the hash function, and thus, does not user a hash-value a. Furthermore, unlike the present invention, Cramer does not rely upon g_1^{a1} in the calculation of v. In this way, for example, Cramer is clearly different from the claimed invention. Specifically, the verification cipher-number v, as calculated in Cramer (i.e., $v = c^r d^{ra}$) is quite different from v, as calculated in the present invention (i.e., $v = g_1^{a1} c^r d^{ar} \ mod \ p$), and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

By way of further example, as shown in column 8, line 5, Cramer discloses the formulas used for calculating u_1, u_2 and v. As shown, Cramer does not disclose the use of modulo arithmetic in the equations used to calculate u_1, u_2 and v. This is quite different from the present invention, where the step of generating a public key includes where the elements u_1, u_2 and v, are calculated using modulo arithmetic. Accordingly, Cramer does not teach generating a public key in the manner claimed, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where $|x|$ is the number of digits of x), selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d^{\alpha r} \bmod p$$

generating a ciphertext C of transmission data m (positive integer) by:

$$e = E_{pk}(\alpha_1 || \alpha_2 || m)$$

by using the secret key, and transmitting (u_1, u_2, e, v) as the ciphertext" as recited in independent claim 41.

Another feature of the present invention, as recited in independent claim 41, includes a ciphertext reception and decipher step. This step includes a condition, such that a step of outputting m' as the deciphered results if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} \equiv v \pmod p$$

If the above condition is not satisfied, then a step of outputting as the decipher results the effect that the received ciphertext is rejected. Cramer does not disclose this feature. To support the assertion that Cramer teaches this feature, the Examiner cites columns 9-11. However, neither the cited text nor any other portions of Cramer teach or suggest the claimed features.

For example, as described in column 8, lines 50-62, Cramer discloses a condition [1]: $u_1{}^{x1+y1a}\ u^{x2+y2a} = v$. The condition [1] of Cramer is not the same as the above-described condition of the present invention. Accordingly, Cramer does not disclose the claimed feature, and the Examiner has not provided any explanation as to why one of ordinary skill in the art would be motivated to modify Cramer to obtain this feature.

Therefore, Cramer fails to teach or suggest "a ciphertext reception and

decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, m' is a positive integer) which satisfy:

$$\alpha'_1||\alpha'_2||m' = D_{sk}(e)$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} \equiv v \pmod{p},$$

where:

$$\alpha' = \alpha'_1||\alpha'_2$$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected" as recited in independent claim 41.

D. Conclusion

Therefore, based on the above remarks, Appellants submit that the Examiner's final rejection of claims 25-27, 29, 31-34 and 37-39 under 35 USC §112, second paragraph; the rejection of claims 23-44 under 35 USC §101; and the rejection of claims 23-44 USC §103(a) are not properly founded in law and respectfully request that the Board of Patent Appeal Interferences reverse the Examiner's final rejection.

To the extent necessary, applicants petition for an extension of time under 37 CFR §1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1417 (Case No. 500.41092X00) and please credit any excess fees to such Deposit Account.

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

Carl I. Brundidge
Registration No. 29,621

CIB/DKM/cmd
(703) 684-1120
Enclosures

VIII. CLAIMS APPENDIX

Claims 1-22 (canceled).

23. A public-key cryptographic method implemented in a computer system comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1}{g_2}^{x_2}$, $d_1 = {g_1}^{y_{11}}{g_2}^{y_{12}}$, $d_2 = {g_1}^{y_{21}}{g_2}^{y_{22}}$, $h = {g_1}^{z}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1,\ \forall \alpha_2 \in X_2)$$

where M is a plaintext space;

a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Zq$ for a plaintext m ($m \epsilon M$), calculating:

$$u_1 = {g_1}^{r}, \quad u_2 = {g_2}^{r}, \quad e = \pi(\alpha_1, \alpha_2, m)h^{r}, \quad v = {g_1}^{\alpha_1} c^{r} {d_1}^{\alpha r} {d_2}^{mr}$$

where $\alpha = \alpha_1 || \alpha_2$, and transmitting ($u_1$, u_2, e, v) as a ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, $m' \epsilon M$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = e / {u_1}^{z}$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+m' y_{21}} u_2{}^{x_2+\alpha' y_{12}+m' y_{22}} = v$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 \,||\, \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

24. A public-key cryptographic method implemented in a computer comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1{}^{x_1} g_2{}^{x_2} \bmod p$, $d_1 = g_1{}^{y_{11}} g_2{}^{y_{12}} \bmod p$, $d_2 = g_1{}^{y_{21}} g_2{}^{y_{22}} \bmod p$, $h = g_1{}^{z} \bmod p$,
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$

a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for a plaintext m ($|m| = k_3$, where $|x|$ is a number of digits of x), calculating:

$$\tilde{m} = \alpha || K$$

selecting a random number $r \in Zq$, calculating:

$$u_1 = g_1{}^{r} \bmod p, \quad u_2 = g_2{}^{r} \bmod p, \quad e = \tilde{m}\, h^{r} \bmod p, \quad v = g_1{}^{\alpha_1} c^{r} d_1{}^{\alpha r} d_2{}^{mr} \bmod p$$

and transmitting (u_1, u_2, e, v) as a ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|m'| = k_3$) which satisfy:

$$\alpha'_1||\alpha'_2||m' = e/{u_1}^z \bmod p$$

and if the following is satisfied:

$${g_1}^{\alpha'_1}{u_1}^{x_1+\alpha' y_{11}+m' y_{21}}{u_2}^{x_2+\alpha' y_{12}+m' y_{22}} \equiv v \pmod p$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 || \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

25. A public-key cryptographic method according to claim 23, wherein the public-key is generated by a receiver and is made public.

26. A public-key cryptographic method according to claim 23, wherein in said ciphertext transmission step, the random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$ and $r \epsilon Zq$ are selected beforehand and the following is calculated and stored beforehand:

$$u_1 = {g_1}^r, \quad u_2 = {g_2}^r, \quad h^r, \quad {g_1}^{\alpha_1} c^r {d_1}^{\alpha r}$$

27. A public-key cryptographic method according to claim 24, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$), and $r \epsilon Zq$ are selected beforehand and the following is

calculated and stored beforehand:

$$u_1 = {g_1}^r \bmod p, \quad u_2 = {g_2}^r \bmod p, \quad h^r \bmod p, \quad {g_1}^{\alpha_1} c^r {d_1}^{\alpha r} \bmod p$$

28. A cryptographic communication method implemented in a computer system comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1} {g_2}^{x_2}$, $d_1 = {g_1}^{y_{11}} {g_2}^{y_{12}}$, $d_2 = {g_1}^{y_{21}} {g_2}^{y_{22}}$, $h = {g_1}^z$,
- $\pi : X_1 \times X_2 \times M \longrightarrow G'$: one-to-one mapping
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- E : symmetric encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

where M is a key space;

a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Zq$ for key data K ($K \epsilon M$), calculating:

$$u_1 = {g_1}^r, \quad u_2 = {g_2}^r, \quad e = \pi(\alpha_1, \alpha_2, K) h^r, \quad v = {g_1}^{\alpha_1} c^r {d_1}^{\alpha r} {d_2}^{Kr}$$

where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by:

$$C = E_K(m)$$

by using a symmetric cryptographic function E and key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, K' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, $K' \epsilon M$) which satisfy:

$$\pi(\alpha'_1 || \alpha'_2 || K') = e / {u_1}^z$$

and if the following is satisfied:

$${g_1}^{\alpha'_1} {u_1}^{x_1 + \alpha' y_{11} + K' y_{21}} {u_2}^{x_2 + \alpha' y_{12} + K' y_{22}} = v$$

where $\alpha' = \alpha'_1 \| \alpha'_2$

executing a decipher process by:

$$m = D_{K'}(C)$$

outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

29. A cryptographic communication method according to claim 28, wherein the ciphertext C is generated by:

$$C = E_K(f(\alpha_1, \alpha_2) || m)$$

by using a symmetric cryptographic function E, the key data K and a

publicized proper function f, it is checked whether the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+K' y_{21}} u_2{}^{x_2+\alpha' y_{12}+K' y_{22}} = v,$$
$$f(\alpha'_1, \alpha'_2) = [D_{K'}(C)]^k$$

where f outputs a value of k bits and $[x]^k$ indicates the upper k bits of x, and if the check passes, a decipher process is executed by:

$$m = [D_{K'}(C)]^{-k}$$

where $[x]^{-k}$ indicates a bit train with the upper k bits of x being removed.

30. A cryptographic communication method implemented in a computer system comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_{11}, y_{12}, y_{21}, y_{22}, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1{}^{x_1} g_2{}^{x_2} \bmod p$, $d_1 = g_1{}^{y_{11}} g_2{}^{y_{12}} \bmod p$, $d_2 = g_1{}^{y_{21}} g_2{}^{y_{22}} \bmod p$, $h = g_1{}^{z} \bmod p$,
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$
- E : symmetric encipher function

a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) for key data K ($|K| = k_3$, where $|x|$ is a number of digits of x), calculating:

$$\tilde{m} = \alpha || K$$

selecting a random number $r \epsilon Z_q$, calculating:

$$u_1 = g_1{}^r \bmod p, \quad u_2 = g_2{}^r \bmod p, \quad e = \tilde{m}\, h^r \bmod p, \quad v = g_1{}^{\alpha_1} c^r d_1{}^{\alpha r} d_2{}^{Kr} \bmod p$$

and generating a ciphertext C of transmission data by:

$$C = E_K(m)$$

by using a (symmetric) cryptographic function E and the key data K, and transmitting (u_1, u_2, e, v, C) as the ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, K' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, $|K'| = k_3$) which satisfy:

$$\alpha'_1 || \alpha'_2 || K' = e / u_1{}^z \bmod p$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1 + \alpha' y_{11} + K' y_{21}} u_2{}^{x_2 + \alpha' y_{12} + K' y_{22}} \equiv v \pmod p$$

where $\alpha' = \alpha'_1 \,||\, \alpha'_2$,

executing a decipher process by:

$$m = D_{K'}(C)$$

outputting deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

31. A cryptographic communication method according to claim 30,

wherein the ciphertext C is generated by:

$$C = E_K(f(\alpha_1, \alpha_2)||m)$$

by using a symmetric cryptographic function E, the key data K and a publicized proper function f, it is checked whether the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_{11}+K' y_{21}} u_2{}^{x_2+\alpha' y_{12}+K' y_{22}} \equiv v \pmod{p},$$
$$f(\alpha'_1, \alpha'_2) = [D_{K'}(C)]^k$$

where f outputs a value of k bits and $[x]^k$ indicates the upper k bits of x, and if the check passes, a decipher process is executed by:

$$m = [D_{K'}(C)]^{-k}$$

where $[x]^{-k}$ indicates a bit train with the upper k bits of x being removed.

32. A cryptographic communication method according to claim 28, wherein the public-key is generated by a receiver and is made public.

33. A cryptographic communication method according to claim 28, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$) and $r \epsilon Zq$ are selected beforehand and the following is calculated and stored beforehand:

$$u_1 = g_1{}^r, \quad u_2 = g_2{}^r, \quad h^r, \quad g_1{}^{\alpha_1} c^r d_1{}^{\alpha r}$$

34. A cryptographic communication method according to claim 28,

wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$) and $r \epsilon Zq$ are selected beforehand and the following is calculated and stored beforehand:

$$u_1 = {g_1}^r \bmod p, \quad u_2 = {g_2}^r \bmod p, \quad h^r \bmod p, \quad {g_1}^{\alpha_1} c^r {d_1}^{\alpha r} \bmod p$$

35. A cryptographic communication method implemented in a computer system comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$

and a public-key:

- G, G' : finite (multiplicative) group $\quad G \subseteq G'$
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = {g_1}^{x_1} {g_2}^{x_2}$, $d = {g_1}^{y_1} {g_2}^{y_2}$, $h = {g_1}^z$,
- $\pi : X_1 \times X_2 \times M \longrightarrow \mathrm{Dom}(E)$: one-to-one mapping (Dom(E) is the domain of the function E)
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- H : hash function
- E : symmetric encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Zq$, calculating:

$$u_1 = {g_1}^r, \quad u_2 = {g_2}^r, \quad v = {g_1}^{\alpha_1} c^r d^{\alpha r}, \quad K = H(h^r)$$

where $\alpha = \alpha_1 \| \alpha_2$, generating a ciphertext C of transmission data m by

$$C = E_K(\pi(\alpha_1, \alpha_2, m))$$

by using a (symmetric) cryptographic function E; and transmitting (u_1, u_2, v, C) as the ciphertext; and

a ciphertext reception and decipher step of calculating:

$$K' = H({u_1}^z)$$

by using the secret key, calculating from the received ciphertext, α'_1, α'_2 (where $\alpha'_1 \epsilon X_1$ $\alpha'_2 \epsilon X_2$) which satisfy:

$$\pi(\alpha'_1, \alpha'_2, m') = D_{K'}(C)$$

if the following is satisfied:

$${g_1}^{\alpha'_1} {u_1}^{x_1 + \alpha' y_1} {u_2}^{x_2 + \alpha' y_2} = v,$$

where $\alpha' = \alpha'_1 \| \alpha'_2$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

36. A cryptographic communication method implemented in a computer system comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2, z \in \mathbb{Z}_q$

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = {g_1}^{x_1} {g_2}^{x_2} \bmod p$, $d = {g_1}^{y_1} {g_2}^{y_2} \bmod p$, $h = {g_1}^{z} \bmod p$,
- k_1, k_2, k_3 : positive constant $(10^{k_1+k_2} < q,\ 10^{k_3} < q,\ 10^{k_1+k_2+k_3} < p)$
- H : hash function
- E : symmetric encipher function (the domain of E is all positive integers)

a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 \,||\, \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where ($|x|$ is the number of digits of x), selecting a random number $r \epsilon Z_q$, calculating:

$$u_1 = {g_1}^{r} \bmod p, \quad u_2 = {g_2}^{r} \bmod p, \quad v = {g_1}^{\alpha_1} c^r d^{\alpha r} \bmod p, \quad K = H(h^r \bmod p)$$

transmitting the ciphertext (u_1, u_2, v, C); generating a ciphertext C of transmission data m by:

$$C = E_K(\alpha_1 || \alpha_2 || m)$$

by using a (symmetric) cryptographic function, and transmitting (u_1, u_2, v, C) as the ciphertext; and

a ciphertext reception and decipher step of calculating:

$$K' = H({u_1}^{z} \bmod p)$$

by using the secret key, calculating from the received ciphertext, α'_1, α'_2 ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$) which satisfy:

$$\alpha'_1 || \alpha'_2 || m' = D_{K'}(C)$$

and if the following is satisfied:

$$g_1{}^{\alpha'_1} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} \equiv v \pmod{p}$$

outputting m' as the deciphered results (where $\alpha' = \alpha'_1 \,||\, \alpha'_2$), whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

37. A cryptographic communication method according to claim 35, wherein the public-key is generated by a receiver and is made public.

38. A cryptographic communication method according to claim 35, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$) and $r \epsilon Zq$ are selected beforehand and the u_1, u_2, e and v are calculated and stored beforehand.

39. A cryptographic communication method according to claim 36, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$), and $r \epsilon Zq$ are selected beforehand and the u_1, u_2, e and v are calculated and stored beforehand.

40. A cryptographic communication method implemented in a computer system comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (asymmetric cryptography) decipher key

and a public-key:

- G : finite (multiplicative) group
- q : prime number (the order of G)
- $g_1, g_2 \in G$
- $c = g_1^{x_1} g_2^{x_2}$, $d = g_1^{y_1} g_2^{y_2}$,
- $\pi : X_1 \times X_2 \times M \longrightarrow \mathrm{Dom}(E)$: one-to-one mapping (Dom(E) is the domain of the function E)
- $\pi^{-1} : \mathrm{Im}(\pi) \longrightarrow X_1 \times X_2 \times M$
- $E_{pk}(\cdot)$: (asymmetric cryptography) encipher function

where the group G is a partial group of the group G', X_1 and X_2 are an infinite set of positive integers which satisfy:

$$\alpha_1 || \alpha_2 < q \qquad (\forall \alpha_1 \in X_1, \forall \alpha_2 \in X_2)$$

where M is a plaintext space;

a ciphertext generation and transmission step of selecting random numbers $\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$, $r \epsilon Zq$, calculating:

$$u_1 = g_1^r, \quad u_2 = g_2^r, \quad v = g_1^{\alpha_1} c^r d^{\alpha r}$$

where $\alpha = \alpha_1 || \alpha_2$, generating a ciphertext C of transmission data m by:

$$e = E_{pk}(\pi(\alpha_1, \alpha_2, m))$$

by using an (asymmetric) cryptographic function E_{pk}, and transmitting (u_1, u_2, e, v) as the ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($\alpha'_1 \epsilon X_1$, $\alpha'_2 \epsilon X_2$, $m' \epsilon M$) which satisfy:

$$\pi(\alpha_1', \alpha_2', m') = D_{sk}(e)$$

and if the following is satisfied:

$$g_1{}^{\alpha_1'} u_1{}^{x_1+\alpha' y_1} u_2{}^{x_2+\alpha' y_2} = v$$

where:

$$\alpha' = \alpha_1' || \alpha_2'$$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

41. A cryptographic communication method implemented in a computer system comprising:

a key generation step of generating a secret-key:

- $x_1, x_2, y_1, y_2 \in \mathbb{Z}_q$
- sk : (asymmetric cryptography) decipher key

and a public-key:

- p, q : prime number (q is a prime factor of p-1)
- $g_1, g_2 \in \mathbb{Z}_p$: $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = q$
- $c = g_1{}^{x_1} g_2{}^{x_2} \bmod p$, $d = g_1{}^{y_1} g_2{}^{y_2} \bmod p$,
- k_1, k_2 : positive constant $(10^{k_1+k_2} < q)$
- $E_{pk}(\cdot)$: (asymmetric cryptography) encipher function (the domain is all positive integers)

a ciphertext generation and transmission step of selecting random numbers $\alpha = \alpha_1 || \alpha_2$ ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$, where $|x|$ is the number of digits of x), selecting a random number $r \epsilon Z_q$, calculating:

$$u_1 = {g_1}^r \bmod p, \quad u_2 = {g_2}^r \bmod p, \quad v = {g_1}^{\alpha_1} c^r d^{\alpha r} \bmod p$$

generating a ciphertext C of transmission data m (positive integer) by:

$$e = E_{pk}(\alpha_1 || \alpha_2 || m)$$

by using the secret key, and transmitting (u_1, u_2, e, v) as the ciphertext; and

a ciphertext reception and decipher step of calculating from the received ciphertext and by using the secret key, α'_1, α'_2, m' ($|\alpha'_1| = k_1$, $|\alpha'_2| = k_2$, m' is a positive integer) which satisfy:

$$\alpha'_1 || \alpha'_2 || m' = D_{sk}(e)$$

and if the following is satisfied:

$${g_1}^{\alpha'_1} {u_1}^{x_1 + \alpha' y_1} {u_2}^{x_2 + \alpha' y_2} \equiv v \pmod p,$$

where:

$$\alpha' = \alpha'_1 || \alpha'_2$$

outputting m' as the deciphered results, whereas if not satisfied, outputting as the decipher results the effect that the received ciphertext is rejected.

42. A cryptographic communication method according to claim 40, wherein the public-key is generated by a receiver and is made public.

43. A cryptographic communication method according to claim 40, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($\alpha_1 \epsilon X_1$, $\alpha_2 \epsilon X_2$) and $r \epsilon Zq$ are selected beforehand and the u_1, u_2 and v are

calculated and stored beforehand.

44. A cryptographic communication method according to claim 41, wherein in said ciphertext transmission step, the random numbers α_1, α_2 ($|\alpha_1| = k_1$, $|\alpha_2| = k_2$), and $r_{\epsilon}Zq$ are selected beforehand and the u_1, u_2 and v are calculated and stored beforehand.

IX. EVIDENCE APPENDIX

There is no evidence relied upon in this Appeal.

X. RELATED PROCEEDINGS APPENDIX

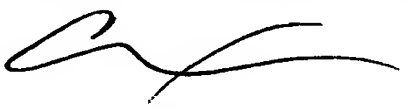
There are no related proceedings.

XI. FEES

To the extent necessary, applicants petition for an extension of time under 37 CFR §1.136. Please charge any shortage in the fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 50-1417 (Case No. 500.41092X00) and please credit any excess fees to such Deposit Account.

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.



Carl I. Brundidge
Registration No. 29,621

CIB/DKM/cmd
(703) 684-1120
Enclosures (in triplicate)